arcserve®

The Role of Unified Data Resilience and Immutable Backups In Ransomware Attacks, Breaches, and Natural Disasters

Table of Contents

What Is a Unified Data Resilience Platform (and Why Do You Need One)?

Ransomware is everywhere. And it's knocking on almost every organization's door. Sophos' The State of Ransomware 2023 found that 66 percent of surveyed organizations were hit by ransomware in the last year, with 76 percent of those attacks resulting in the victim's data being encrypted.

The same report found the associated costs of an attack are astronomical, with the average ransom coming in at $1.54 million and the mean recovery cost, excluding ransom payment, $1.82 million.

But ransomware isn't the only threat to your business and your data. According to Forbes, in 2022, the United States experienced 18 large-scale climate disasters that in total damage cost the country $175.2 billion. You can bet that IT and data recovery comprise a substantial enough portion of those costs that hundreds, if not thousands, of businesses took a huge financial hit. Given the costs of a disaster—whether it's a hurricane or a data breach—ensuring your organization is resilient is common sense.

Backups Are a Big Target

Clearly, recovery using backups is considerably cheaper than the costs of a data disaster. But backups are a primary target because once the hacker encrypts them, your chances of recovery may be limited. One study found that in 21 percent of ransomware attacks, backups were targeted and rendered entirely useless. And sometimes, the recovery costs may be higher than the ransom itself.

There Is No Silver Bullet

If you're an IT pro responsible for your organization's IT resilience, you already know there is no single solution guaranteed to keep your organization and data secure. You need to employ a multi-modal strategy to achieve cyber and data resilience.

Implement Data Resilience Technologies and Processes

That starts with instituting processes and employing technologies that strengthen your security posture. Employee cybersecurity training should be an ongoing process, given that, according to the Verizon 2023 Data Breach Investigations Report, 74 percent of breaches involve the human element.

And regularly scheduled disaster recovery tests and exercises should be executed to ensure recovery is possible—before it's needed. The Cybersecurity and Infrastructure Security Agency (CISA) is a great starting point, offering disaster recovery consultation, documentation, and testing services.

Strengthen Your Cybersecurity Measures

You'll want to institute added layers of security to protect your data, including employing identity and access management (IAM) to block unauthorized users. IAM can include single sign-on systems, two-factor authentication, multifactor authentication, privileged access management (PAM), and role-based access controls (RBACs). You'll see that MFA isn't perfect if you read this recent post. However, protections minimize the chances that an unauthorized user can access your network.

Choose a Unified Data Resilience Platform

The National Institute of Standards and Technology (NIST) Cybersecurity Framework calls for a multi-model approach to ensuring business and data resilience. We've built the Arcserve Unified Data Resilience platform to help you get there. That platform is built on three pillars that ensure your data is safeguarded and can always be recovered.

Prevent

Arcserve's partnership with cybersecurity leader Sophos means your backups are protected with Sophos Intercept X Advanced for Server, cutting-edge cybersecurity that uses a deep learning neural network to detect known and unknown malware—without relying on signatures. And you can quickly respond to and remove threats with CryptoGuard, which constantly monitors file writes for encrypted files, and WipeGuard, which uses behavioral analysis to stop never-before-seen ransomware and boot-record attacks.

Protect

Because prevention isn't foolproof, the Arcserve platform's second pillar is protection. Regardless of the cause—external threats, disasters, human error, or unplanned outages—Arcserve offers solutions that protect your physical and virtual on-premises, cloud, and SaaS-based data.

We've forged a foundation for data resilience and backup protection that features immutable storage, a write-once-read-many-times format that can't be altered or deleted. That includes support for Amazon Web Services (AWS) S3 Object Lock. And we protect your data with robust encryption, air gap support, IAM and PAM controls, and more.

Recover

The Arcserve Unified Data Resilience platform makes the most significant difference for you when you need it most—after a successful ransomware attack or another data disaster. Arcserve solutions let you safely spin up copies of physical and virtual systems onsite and offsite or in private and public clouds. That makes near-instant recovery possible and ensures business continuity.

Arcserve: Spanning the Entire Business Continuity Category

At Arcserve, we're proud to say that we provide the broadest set of best-in-class solutions to manage, protect and recover all data workloads, from SMB to enterprise and regardless of location or complexity. That covers a lot of ground. Watch for a future post where we'll tour Arcserve products and solutions and show you how each amplifies the power of our Unified Data Resilience platform.

Since IT teams are typically burdened by daily demands to keep operations moving while supporting business innovation, expert help can go a long way toward becoming a genuinely resilient organization.

Talking to an Arcserve technology partner here.

5 Ways Immutable Backups Strengthen Your Company's Data Resilience and Why #1 Matters Most)

Your business lives and dies by its data. That's probably no surprise, with Statista saying the amount of data created, captured, copied, and consumed globally will reach 120 zettabytes this year.

Let's consider what comprises your data. Start with the basics: email. Again according to Statista, we are projected to send 347.3 billion emails in 2023. Hackers employ emails to infiltrate your network using phishing, malicious attachments, or other means. But your business relies on data that may be even more precious than email. Think financial records, private customer data, and partner information.

So, while an attack can start with an email, once inside your network, the hackers will try to expand the attack wherever possible, encrypting files—including your email servers and critical databases—along the way. That's where immutable backups make all the difference in the world. Here are five ways they do so.

1. Immutable Backups Are Immune From Attacks

Immutable backups are copies of your data that are saved in a write-once-read-many-times (WORM) format that can't be altered, tampered with, or deleted by unauthorized users—even if they gain access to your primary data and backup systems. That's why we recommend you follow the 3-2-1-1 backup strategy. That last "1" means you should keep one copy of your data in immutable storage where it's safeguarded from malicious attacks, accidental deletions, and any other type of data loss, making immutability a core component of your data resilience strategy.

2. Insider Threats Are Mitigated

Whether an insider tampers with or deletes any of your data intentionally or accidentally, the results can be the same: expensive. Employees with access to critical data can create a data disaster in a few clicks. Immutable backups give you an added safety net, ensuring that you always have a usable copy of your data that lets you quickly recover and get back to business.

3. Compliance Is Less Complicated

Compliance with government edicts like the General Data Protection Regulation (GDPR) in the EU and California Consumer Privacy Act (CCPA) in the United States can be vital to your company's success. Immutable backups are crucial in meeting those requirements by providing an immutable data record.

4. Disaster Recovery Is Ensured

Arcserve OneXafe offers immutable network-attached storage and continuous data protection by taking a snapshot every 90 seconds. Each snapshot always creates a new object, preserving a view of the file system at the instant the snapshot is taken. Since the underlying objects are immutable, the snapshots inherit that immutability. Your data is preserved and protected, but just as importantly, snapshots let you go back to specific points in time and recover entire file systems in minutes.

5. Data Integrity Is Assured

Immutability gives you a mechanism for verifying your data's integrity. Because your immutable backups can't be altered, they can be compared to your original data so you can confirm that no changes have occurred. While immutability is your last line of defense, we've simplified ensuring all your backups are recoverable by including Arcserve Assured Recovery with Arcserve Unified Data Protection (UDP).

Assured Recovery enables automated disaster recovery testing of your business-critical systems, applications, and data. It lets you test the integrity of data on your replica server. Arcserve UDP replicates backup data by saving it as recovery points from one server to another recovery point server. You can also create virtual machines from the backup data that can act as standby machines when the source node fails.

Data Resilience Starts With Immutability

We've made the case for including immutable backups as a priority in your disaster recovery strategy. If you aren't already using immutable backups, talking to an Arcserve technology partner is an excellent place to start. They can help you understand your options, identify the right solution for your business, and implement an effective data resilience strategy. Find an Arcserve technology partner here.

5 Steps Every Organization Should Take to Bolster Data Resilience (and Why #5 May Matter Most)

If you're like most other IT pros, doing everything possible to fight against cyberattacks and ransomware and ensure data resilience is probably your first priority.

One step in that direction is the adoption of multifactor authentication (MFA). According to a recent Okta survey, 64 percent of users are authenticated using MFA as of January 2023, and MFA is used by 90 percent of administrators.

That's why this recent PCMag headline caught our eye: Has Multi-Factor Authentication Failed Us?. The article's subhead explains that, even with the growth of MFA, data breaches continue to increase. A recent survey from Check Point Software proves the point, finding that global attacks rose seven percent in the first quarter of 2023, with each organization surveyed facing an average of 1,248 attacks per week.

MFA: Your First Line of Defense

First and foremost, we firmly believe that MFA is a valuable tool for ensuring data resilience. But it isn't perfect. The PCMag article refers to the Verizon 2023 Data Breach Investigation Report, which found that 83 percent of attacks involve the human element. That comes into play as individuals and admins can be tricked, and vulnerabilities can be exploited even when MFA is being used.

The Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory that affirms that MFA is one of the most essential cybersecurity practices you can employ to reduce the risk of intrusions, noting that users who enable MFA are 99 percent less likely to have an account compromised.

MFA Can Be Exploited

The CISA advisory also shares the story of an MFA exploit from May of last year that is telling. It describes how Russian state-sponsored cyber actors had gained network access by exploiting default MFA protocols—by taking advantage of a misconfigured account set to default MFA protocols—at a non-governmental organization (NGO).

That allowed the hackers to enroll a new device for MFA and access the victim's network. The actors then exploited a critical Windows Print Spooler vulnerability, "PrintNightmare" (CVE-2021-34527), to run arbitrary code with system privileges. That enabled access to cloud and email accounts for document exfiltration.

Another attack involving MFA protections for a Sitel customer service agent account occurred in January 2022. The Okta Security team was alerted that a new factor was added to a Sitel customer support engineer's Okta account. While the problem began with Sitel, Okta estimated that nearly 1,000 credentials across more than 130 companies were stolen directly from companies or through subsequent breaches.

And in September 2022, an Uber EXT contractor's account was compromised by what's called "MFA Fatigue." That's where the hacker keeps prompting the user to approve the authentication until they simply OK the request to make it disappear. According to Uber, it worked, with the attacker accessing several other employee accounts—which ultimately gave the attacker elevated permissions to several tools, including G-Suite and Slack.

Why You Need to Add a Last Line of Defense

Once an attacker gets into your systems, they can wreak havoc. The first response is to shut down networks and systems to prevent further exploitation and start recovery. But that is a very costly decision.

The Uptime Institute's 2022 Outage Analysis found that 80 percent of data center operators and managers had experienced some type of outage in the past three years. And most organizations can only guess how much that downtime costs in dollars and damage to their reputations—until it happens. Meanwhile, an IBM study found that the average cost of a data breach in the United States is $9.44 million.

Add it all up, and it's clear that a comprehensive approach to data resilience is your best bet for overcoming vulnerabilities, whether they result from hacker MFA workarounds or a successful ransomware attack.

That includes adhering to the 3-2-1-1 backup strategy, with one copy of your backups in immutable storage, a write-once-read-many-times format that can't be altered or deleted. And unlike data encryption, there is no key, so there shouldn't be any way to "read" or reverse the immutability. An immutable copy of your data is impervious to ransomware infections.

Arcserve gives you plenty of proven options that add a last line of defense to ensure your data is always safeguarded, resilient, and recoverable.

Unified Data Protection: Protection, Prevention, and Recovery

It takes a comprehensive approach to data protection to ensure data resilience. That's precisely what Arcserve Unified Data Protection (UDP) delivers, with an all-in-one data solution that neutralizes ransomware attacks, makes it easy to restore your data, and performs effective disaster recovery.

Arcserve UDP is safeguarded by Sophos Intercept X Advanced cybersecurity, uniquely combining deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity for multilayered, complete IT resilience, protecting against data loss and extended downtime across your cloud, local, virtual, hyperconverged, and SaaS workloads.

With Arcserve UDP, you can reduce your downtime from days to minutes and validate recovery time and recovery point objectives (RPOs/RTOs) and service-level agreements (SLAs) with automated testing and granular reporting.

Some MFA breaches have resulted in ransomware, including an attack on Cisco. Arcserve UDP ensures your backups are protected when saved in immutable format, thanks to support for Amazon S3 Object Lock in the cloud and onsite and offsite immutable storage, including integration with Arcserve OneXafe immutable network-attached storage appliances.

Talk to the Data Resilience Experts

Besides serving customers, Arcserve Technology Partners spend their days staying up-to-date on the latest threats, vulnerabilities, and technologies that ensure data resilience.

Take advantage of their experience by choosing an Arcserve partner here. To learn more about Arcserve UDP, request a demo.

Achieving Data Resilience with Immutable Data Storage in Multi-Cloud Environments

From an organizational perspective, Gartner says that coupling radical efficiency with innovation to drive business resiliency, growth, and profits requires shrewd investing in digital. That's because a resilient business delivers better bottom-line results: McKinsey found that from 2020 through 2021, resilient companies generated shareholder returns that were 50 percent higher than those of less resilient peers.

And that explains why in today's world—rife with threats coming at businesses from every direction—data resiliency is the top priority for every IT pro. That's especially true in complex, multi-cloud environments. A recent independent study of IT decision-makers, commissioned by Arcserve, bears this out, with 83 percent of respondents saying their organization includes data resilience in their strategies.

If your business relies on multiple clouds, achieving data resiliency starts with ensuring your data is protected everywhere. That's where immutable storage comes into play.

What Is Immutable Data Storage?

When your data is placed in immutable storage, it's converted into a write-once-read-many-times (WORM) format that can't be altered or deleted. TechTarget says data stored in an immutable format "will remain completely static and pristine for its entire existence (and) can never be tampered with, modified, or removed." That means your immutable stored data is protected against accidental or malicious changes, deletions, or corruption.

Immutability Brings Crucial Benefits to Multi-Cloud Environments

With your data backed up in immutable storage, it's not only protected, but it also helps you meet regulatory requirements and facilitates compliance audits. That's especially helpful in heavily regulated industries, such as healthcare and finance, where immutable storage offers an audit trail, ensuring transparency and accountability.

Most importantly, your immutable backups ensure you can always restore your data, even if you're struck by ransomware, a hardware failure, or even a natural disaster. So, how do you leverage immutable storage and achieve data resiliency in multi-cloud environments—without adding more complexity?

Arcserve UDP: The Multi-Cloud Data Resiliency Solution

In a multi-cloud environment, you need more than cloud data protection. You need unified protection and cyberattack prevention across all of your infrastructure—on-premises, off-premises, and in the cloud.

That's where Arcserve Unified Data Protection (UDP) is a game-changer, delivering complete IT resiliency for your virtual, physical, and cloud infrastructures and SaaS-based workloads. Arcserve UDP protects against data loss and reduces downtime from days to minutes. The software also validates recovery time and recovery point objectives (RTOs/RPOs) and service-level agreements (SLAs) and offers automated testing and granular reporting.

Data protection starts with ransomware prevention. Arcserve delivers on that promise with available Sophos Intercept X Advanced for Server to protect your backup infrastructure from ransomware. At the same time, immutable cloud storage with AWS Object Lock safeguards your data and repels hacker attacks. And Arcserve UDP fully protects a broad range of SaaS platforms.

Scale Easily Across Your Infrastructure

With Arcserve UDP, you can quickly scale hybrid business continuity topologies, locally or over long distances, with multiple sites, including service and cloud providers. And installation is done in a few clicks.

You can quickly create data stores on the recovery point server, add the nodes you want to protect, a storage destination, and a plan. And it's easy to perform jobs such as backup, virtual standby, replication, or even a simple restore or a bare metal recovery.

Arcserve UDP lets you back up to either a local machine or a central recovery point server (RPS) with global, source-side deduplication. A destination can be an RPS, local folder, or remote shared folder. It's also easy to add network CIFS/NFS shares, Office 365 Exchange, or SharePoint online nodes and create related tasks.

Data Management Made Easy

You can manage Arcserve UDP with either the on-premises private or cloud-based management console. Long used on-premises by IT pros, the private management console is a good choice if your environment requires a private setting. The cloud-based management console is perfect if you need more flexible controls, such as multitenancy.

Multitenant management is simplified with the cloud-based management console, so you can easily configure sub-organizations, manage them like different tenants, and separate workloads into different domains for easier management. And you get granular security with flexible management capabilities using tenant-level security and storage controls.

Talk to an Arcserve Technology Partner

Get expert guidance and support in creating a more resilient company by choosing an Arcserve technology partner. Find a complete list of our partners here. To learn more about Arcserve UDP, request a demo or check out our 30-day free trial.

Need Answers?

Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792

arcserve.com